Jordan K. Cameron (12051)
jcameron@djplaw.com
DURHAM JONES & PINEGAR, P.C.
3301 N Thanksgiving Way, Suite 400
Lehi, Utah 84043
Telephone: (801) 375-6600
Fax: (801) 375-3865

Attorneys for Plaintiff XMission, L.C.

UNITED STATES DISTRICT COURT
DISTRICT OF UTAH, CENTRAL DIVISION

XMISSION, L.C., a Utah company, Plaintiff, vs. CLICK SALES, INC (dba CLICKBANK), a Delaware Corporation, DOES 1-20, Defendants.	**DECLARATION OF PETER L. ASHDOWN IN SUPPORT OF MOTION FOR ENTRY OF TEMPORARY RESTRAINING ORDER AND PRELIMINARY INJUNCTION (REDACTED)** Case No.: 2:17cv01287 EJF Judge Evelyn J. Furse

I, Peter L. Ashdown, being first duly sworn and having personal knowledge of the Matters asserted herein, do hereby declare as follows:

1. I am the founder of XMission, L.C.

2. I am currently the Chief Technical Officer and President of XMission.

3. I founded XMission in 1993 as Utah's first Internet Service Provider ("ISP"). On October 6, 1993, I filed the Articles of Organization of XMission, L.C. with the State of Utah. A true and correct copy of the *Articles of Organization* is attached hereto as Exhibit 1.

4. Since its inception in 1993 until today, XMission's operation as a *bona fide* business has been well documented. *See* Exhibits 2, 3, 4, 5 and 6 hereto.

5. XMission has maintained business formalities. *See* true and correct copies of (1) Certificate of Existence, August 28, 2015; (2) Article of Amendment, October 31, 1995; (3) Annual Report, November 8, 1995; (4) Operating Agreement, January 1, 1996; (5) Articles of Amendment, August 26, 1996; (6) Annual Report Renewal Form, 2002; (7) Annual Renewal Form, 2003; (8) Change of Address, December 3, 2007; (9) an Amended and Restated Operating Agreement, April 27, 2007; and (10) Certificate of Amendment, February 25, 2008, attached hereto as Exhibit 2.

6. From its early days as a private, Utah ISP, to its current role as a global business Internet provider, XMission has expanded its technical offerings to include sophisticated cloud hosting, web hosting, e-mail service and hosting, collaboration tools, business VoIP phone service, and high speed Internet connectivity solutions including optical Ethernet, copper and fiber. Exhibit 3 hereto is a true and correct summary of XMission's Internet based services as well as the bandwidth usage for each. Throughout its history, XMission has also worked with hundreds of Utah's nonprofit organizations by providing free services, and by sponsoring a variety of community-based events and facilities. [redacted]

7. XMission has been the subject of a significant number of media releases. *See* Exh. 4 hereto; *see also* Exhibit 5 hereto, which is a true and correct list of XMission's significant media coverage relating to its business operations.

8. In cooperation with Salt Lake City government, XMission provides free WiFi to the downtown Salt Lake City metropolitan area. Exhibit 6 hereto is a true and correct Google Maps image showing XMission Wireless Hotspots in Salt Lake City.

9. XMission is a widely known and well-recognized ISP in Utah.

10. As of the date of the emails in question, XMission has had, on average, 37 employees.

[redacted] As of the date of the emails in question, XMission owned and continues to own all the servers, routers, and switches on its network through which it hosts and provides its Internet access services for its customers. [redacted]

12. Consistent with its mission to provide the best Internet services possible, XMission has invested in a sophisticated data center and an efficient cooling system to improve the proficiency of its equipment. Exhibit 9 hereto is an XMission blog post, wherein it explains the data center cooling improvements. [redacted]

13. Throughout its existence, XMission has had to consistently update, upgrade and augment its expansive network and infrastructure in order to combat ongoing spam problems. [redacted]

14. At the time of the emails in question, and continuing to date, XMission was/is the sole owner of all its hardware, and has complete and uninhibited access to, and sole physical control over, the hardware.

15. XMission has always provided Internet access services to both commercial and residential customers.

16. The email accounts hosted and served by XMission include email accounts owned by third-party customers of XMission, email accounts owned by employees and/or customers of XMission's third-party customers, email accounts owned by employees of XMission, and also email accounts owned by XMission itself.

17. At the time of the emails in question, XMission's network consisted, on average, of approximately 50,000 mail accounts with approximately 13,000 billable entities.

18. Based on financial data that I personally reviewed, throughout its business history, XMission has expended well in excess of [redacted] in hardware acquisition, maintenance and related expenses to increase capacity to deal with increased spam and related harm, spam filtering expenses, and employee time in dealing with problems caused by its receipt of spam generally. This financial data can be provided upon request of the Court.

19. XMission expends, on average, roughly [redacted] per year in dealing with spam related issues and associated employee time, exclusive of attorney fees. This financial data can be provided upon request of the Court.

20. At the time of the emails in question, XMission had two full-time employees whose primary responsibilities was to deal with spam related issues, including, adjust filtering, responding to customer complaints, addressing blacklist issues, and acting as first responders to data security breaches, and hardware issues caused by spam. Exhibit 13 hereto is a true and correct copy of the job description of XMission's Assistant Mail Systems Administrator, its Mail Systems Administrator, and its Systems Administrator.

21. At the time of the emails in question, XMission employed, on average, 12 other technicians and one supervisor who dedicate at least part of their time to dealing with the aforementioned spam issues.

22. During the time of the emails in question, XMission had 13 servers dedicated specifically to process spam. Those servers could be dedicated to providing XMission's Internet access services if it were not for the spam. XMission has had more total spam-mitigation servers over its history that have crashed or otherwise failed.

[redacted]

[redacted]

25. Once XMission accepts the email, it is handed off to the user's mailbox. There are different systems depending on the type of user, but they all have a default spam score when, if exceeded, the message is not delivered to the Inbox. One system has a quarantine that is entirely separate from their mail account, another uses the Junk folder, etc. Users can also vary what spam score triggers this action. If the spam score is not high enough to automatically be filtered on the user's end, users have individual filter setting that it can use to automatically detect for spam, mark a message as spam or complain about a message as unwanted spam.

XMission also maintains a server for auxiliary spam functions called Mailhub. Mailhub is where reported spam is stored, manually sorted by technicians, at significant expense to XMission, and then processed into the Bayes statistical filter on sadb. Mailhub is also used as a testing server for new SpamAssassin rules, and is where configurations for the mail system in general are centralized. RBL and SURBL lists are maintained on XMission server, postmaster. XMission also stores spam-related statistics for purposes of improving its spam filtering capabilities.

When large numbers of spam emails are not rejected and arrive on XMission's servers and share common data, such as sender domains, IP Addresses, tracking information, etc. those emails are manually reviewed by technicians and attorneys, at significant expense to XMission, to determine how the e-mails are bypassing servers, who is responsible for the e-mails, and whether the e-mails contain violations of the CAN-SPAM Act. If it is determined that the emails contain violations of the CAN-SPAM Act, all data is preserved and XMission pursues its legal remedies available to it through the CAN-SPAM Act. If the emails do not contain violations of the CAN-SPAM Act, XMission does not pursue legal action.

26. At the time of the emails in question, spam occupied on average 12% of all general technical support staff and 39% of mail administrative time.

27. During the same time frame, daily between 40% and 85% of the email messages that passed through XMission's first line of defense and which XMission receives on its system were spam emails, of which the subject emails are a part. Between 2015 and present, the average daily spam amount was around 50% of all email hitting XMission systems. XMission rejects a significant number of spam messages as part of its first line defense. Exhibit 14 hereto is a true and correct summary of data in chart form that shows the percentage of total emails received by XMission that are rejected, categorized as spam, or that are categorized as ham. "Ham" means non-spam emails.

28. Exhibit 15 hereto is a true and correct summary of data in graph form that shows the total volume of emails received by XMission based on category.

29. Exhibit 16 hereto is a true and correct summary of data in chart and graph showing the total daily hours all XMission servers dedicate to processing and filtering spam.

30. The data compilations found in Exhibits 14 through 15 are derived from the data found in XMission's email log which is kept in the ordinary course of business.

31. The number spam received by XMission and its customers would be significantly

higher if not for all the precautions that XMission has taken, including subscribing to leading anti-spam services, including blacklists such as URIBL and Spamhaus, in addition to creating customized and proprietary filtering rules and e-mail server configurations utilizing tools such as SpamAssassin. Exhibit 17 hereto is a detailed graphic prepared by XMission to show how incoming emails are processed by XMission before being delivered to individual inboxes.

32. When an email arrives on XMission's mail servers, it receives a header stamp by one of XMission's incoming SMTP (mail) servers.

33. XMission's incoming mail servers are identified as [redacted]

34. The servers are collectively referred to as mx0x.

35. Nearly every email received on XMission's network is stamped with "mx0x.mta.xmission.com", which indicates that the e-mail was in fact received by one of XMission's mail servers.

36. The server number [redacted] identifies which of XMission's servers received and processed the e-mail.

37. Therefore, an actual received stamp will appear as [redacted] respectively.

38. In rare occasions, an incoming email will be received by one of XMission's backup servers and will not receive a header stamp of mx0x.mta.xmission.com, but instead, a stamp similar to [redacted] A specific example would be [redacted] A review of the emails indicates that a very small number received this type of header stamp as opposed to the typical mx0x.mta.xmission.com stamp.

39. During the time frame in question, XMission received 116,000 emails that were

of a commercial nature and sent by or on behalf of Clickbank. Since the emails were received, they have been stored on XMission's secure servers in their original format and have not been altered in any way.

40. These emails have adversely affected XMission and have contributed to an overall spam problem.

41. Each of the emails is a commercial message and contains commercial content.

42. Each of the 116,000 emails contains a similar header stamp which indicates that it was received by one of XMission's mail servers in Utah.

43. Each of the emails in question contains redirect links that ClickBank calls "HopLinks."

44. A redirect link or HopLink is not a direct path to a specific landing page, but rather consists of a series of links used by marketers and e-mail publishers to track emails for a variety of purposes, including cost-per-click compensation, marketing analytics, to name a few.

45. Redirect links or HopLinks are not visible to the recipient, but instead can only be deciphered by recording a series of transactions that are initiated once a link in the email is clicked.

46. In other words, if a link to an advertisement in an email is clicked (which is often presented as a graphic or hypertext), it will send the recipient on an instantaneous jump through various links which each gathering data or recording information before arriving at the landing page. However, the recipient will simply click the link and believe that they have arrived at the landing page immediately.

47. XMission's Terms of Service, which are available online at

https://xmission.com/legal_terms, provide that "XMission may take action on [customers'] behalf to mitigate spam and [customers] grant to XMission the authority and right to opt-out and/or unsubscribe from receiving any and all spam emails, sent by any party to your email address(es)."

48. In order to attempt to locate the party responsible for the emails, XMission recorded the redirect links. Every one of them contained a redirect links such as clickbank.com and/or clickbank.net through which Clickbank is identified as the responsible party. Exhibit 18 hereto is a sampling of HopLinks from the emails in question. XMission has a report showing the full list of HopLinks for every email in question, but it exceeds 42,000 printed pages. XMission can provide it upon request.

49. Given the enormous amount of emails, and in order to get the emails to stop, XMission has used an automated system to attempt to click on available unsubscribe links in each of the received emails. Such does not appear to have had any effect.

50. From this exercise, XMission has concluded that the majority of the unsubscribe links do not permit the recipient to simply click the link in order to opt-out or require that the recipient take additional steps in order to actually opt-out.

51. As part of its effort to determine the source of the emails and to get them to stop, XMission analyzes the header information and other transmission data that accompanies the emails.

52. To analyze header information, XMission, in part, analyzes the email "from" names designated by the transmitting party and performs a WHOIS look-up in publicly available WHOIS database, to gather contact information associated with the sender domain.

53. The WHOIS database is an online repository of information associated with registered domain names. It stores and publicly displays domain name information, such creation and expiration dates, the registrar of record, and its various contacts (registrant, billing, administrative, and technical).

54. The sender domain is the email domain (e.g @example.com) that was identified as the email domain from which the email was sent.

55. Here, at least 40,506 of emails received through the date of the *First Amended Complaint* contained header information that was false or misleading, and did not readily identify the actual source of the email. These emails used false or generic "from" names and were accompanied by false or concealed WHOIS information thereby impeding XMission's ability to identify the actual source of the email. *See id*.

56. For example, to date, 1,137 were transmitted from the domains: gomatel.us; ewoomy.us; easonto.us; yuws.us; hty00.us; rilkii.us; itshog.us; boyagon.us; ghnnn.us; tree45.us; hptko.us. *See* Exhibit 19, which is a true and correct data compilation showing all the number of emails sent to XMission by these domains. The WHOIS information for these domains identifies Sarah Newville.

57. Exhibit 20, hereto are true and correct copies of three sample emails which are representative samples all of the other 1,137 emails at issue.

58. None of the emails identified Sarah Newville in the "From" but instead, the "From" uses the name "Becky Watson". The emails promote a generic vision restoration trick, and fail to identify any sender in the email. *See* Exh. 20.

59. The emails contain HopLinks.

60. When the HopLinks in the emails are clicked, they route to a landing page controlled by Clickbank for an offer called Quantum Vision System. The landing page states, "ClickBank is the retailer of products on this site. CLICKBANK® is a registered trademark of Click Sales, Inc. . . . located at 917 S. Lusk Street, Suite 200, Boise Idaho, 83706"

61. Notably, neither Clickbank nor Quantum Vision System is identified anywhere in the emails' "from" lines or bodies. *See* Exh. 20.

62. The physical address in the bodies of the emails is 2344 Mason Ave, Porter Ranch, CA 99220. *See* Exh. 20.

63. In another example, 158 were sent from domains with registration information that includes the address Tiroler Str. 24, Lienz, Tirol 9900 Austria. *See* Exhibit 21, which is a true and correct data compilation showing all the number of emails sent to XMission by these domains. Each of these domains was purportedly registered by Armida Stout, with the address Tiroler Str. 24, Lienz, Tirol 9900.

64. Upon examination, this is an address for McDonald's. *See* *https://www.yelp.com/biz/mcdonalds-lienz-osttirol*.

65. None of the emails identified Armida Stout in the "From" and none of the emails promoted McDonald's. Exhibit 22, hereto which are true and correct copies of three sample emails which are representative samples all of the other 158 emails at issue.

66. Rather, the emails promote other products such as de-cluttering techniques and are signed by Marie Gracia Get Organizes Now!. For example, 139 of the emails utilized the "from" name "Remove-Clutter-Now." *See* Exh. 22.

67. A search of publicly available trademarks on file with the U.S. Patent and Trademark Office indicates that there is no registered trademark for "Remove-Clutter-Now". *See* *http://tmsearch.uspto.gov/bin/showfield?f=toc&state=4802%3Aoe9dni.1.1&p_search=searchss&p_L=50&BackReference=&p_plural=yes&p_s_PARA1=&p_tagrepl~%3A=PARA1%24LD&expr=PARA1+AND+PARA2&p_s_PARA2=remove-clutter-now&p_tagrepl~%3A=PARA2%24COMB&p_op_ALL=AND&a_default=search&a_search=Submit+Query&a_search=Submit+Query*.

68. Similarly, A Google search for "remove-clutter-now" does not return one specific brand or product. Rather, it returns a smattering of blog posts, self-help articles, and other information unrelated to the purpose of the email. *See* Exhibit 23, which is a screenshot of Google Search result for "remove-clutter-now."

69. Based on my research, I conclude that the phrase "remove-clutter-now" is generic and does not adequately identify any person who actually transmitted the email.

70. These emails contain HopLinks.

71. When the HopLinks in the emails are clicked, they route to a landing page controlled by Clickbank for an offer called GoodBye Clutter. The landing page states, "ClickBank is the retailer of products on this site. CLICKBANK® is a registered trademark of Click Sales, Inc. . . . located at 917 S. Lusk Street, Suite 200, Boise Idaho, 83706."

72. Clickbank is not identified anywhere in the emails' "from" lines or bodies. *See* Exh. 22.

73. The physical address in the bodies of the emails is 677-3644 Faucibus St. Cork, Ireland. *See* Exh. 22. A Google Maps search indicated that this address is invalid. *See*

https://www.google.com/maps/search/677-3644+Faucibus+St.+Cork,+Ireland/@51.8959999,-8.4980692,13z/data=!3m1!4b1.

74. Many other emails follow this pattern of using generic, false and/or misleading names and registration information in order to prevent the recipient, in this case XMission, from identifying the source of the email.

75. Through its research, XMission has determined that 43,757 emails were sent from sender domains registered with eNom, Inc., GoDaddy, and Mark Monitor.

76. Each of these domain registrars maintains anti-spam policies.

77. Each of the anti-spam policies is available to the public online.

78. In registering 601 domains with eNom, Inc., the registrants represented they did not intend to use them to transmit unsolicited email, as required by the anti-spam policy. In fact, the Defendants did intent to use the domains for this purpose, and did use them for this purpose. Utilizing the falsely obtained domains, Clickbank publishers, acting at Clickbank's direction, and for the promise of a commission payment from Clickbank, sent 28,940 spam emails as part of an unsolicited email campaign to XMission's servers.

79. In registering 160 domains with GoDaddy.com, the registrants represented they did not intend to use them to transmit unsolicited email, as required by the anti-spam policy. In fact, the Defendants did intent to use the domains for this purpose, and did use them for this purpose. Utilizing the falsely obtained domains, Clickbank publishers, acting at Clickbank's direction, and for the promise of a commission payment from Clickbank, sent 10,862 spam emails as part of an unsolicited email campaign to XMission's servers.

80. In registering 8 domains with MarkMonitor, Inc., the registrants represented they did not intend to use them to transmit unsolicited email, to engage in any spamming, or to use distribution lists which include persons who have not specifically given their consent to be placed on such a distribution list, as required by the anti-spam policy. In fact, the Defendants did intent to use the domains for these purposes, and did use them for these purposes. Utilizing the falsely obtained domains, Clickbank publishers, acting at Clickbank's direction, and for the promise of a commission payment from Clickbank, sent 3,955 spam emails as part of an unsolicited email campaign to XMission's servers.

81. In total, 43,757 of the emails received through the date of the *First Amended Complaint* were sent from sender domains that were obtained through false or misleading representations.

82. XMission further analyzes the content in the body of the emails to determine the identity and contact information for the sender.

83. Based on XMission's investigation to date, it appears that none of the emails in question include a proper physical address of the "sender" of each of the emails.

84. For each e-mail at issue in the lawsuit, XMission had to expend man hours and work to identify the source, to examine the transmission information, to examine and analyze the header information, to take efforts to determine how and why the specific e-mails were able to circumvent and/or bypass preliminary filtering techniques, and to ultimately attempt to make the e-mails stop.

85. One of XMission’s competitive advantages is that is has historically been able to offer and Internet access and business hosting services with greatly reduced spam traffic.

86. However, in recent years, spammers have become adept at bypassing spam filtering techniques.

87. The emails in question are emails that, through technology, or other means, have been able to bypass XMission's spam filtering.

88. The spam emails received through the date of the *First Amended Complaint* resulted in 29,796 customer reports of spam pertaining to the emails identified herein, which XMission considers as customer complaints.

89. The emails are continuing to date, and nearly 2,000 of the customer reports of spam came in the weeks leading up to XMission seeking this injunction.

90. In fact, around 60% of the Clickbank emails received on XMission's servers in July 2018 have generated customer reports of spam.

91. In addition to specific customer complaints related to the Clickbank emails, XMission’s reputation and competitive advantage has been harmed, and will continue to be harmed, because customers have taken notice, and continue to take notice of the spam they are receiving to their email addresses.

92. If the emailing is allowed to persist, it will result in possible loss of customers, and a significant, and likely irreparable, damage to XMission’s reputation and competitive advantage in the market place.

93. In summary, the harm XMission suffered, and continues to suffer, as result of the ongoing spam problem, is manifested in financial expense and burden significant to XMission; lost employee time; lost profitability; the necessity to purchase and dedicate equipment

specifically to process spam that could otherwise be dedicated providing Internet access services; harm to reputation; harm to XMission's goodwill; and customer and e-mail recipient complaints.

I declare under penalty of perjury of the laws of that State of Utah and the United States of America that the foregoing is true and correct to the best of my knowledge.

EXECUTED this 13th day of July 2018.

/s/ Peter L. Ashdown
Peter L. Ashdown

(* I certify that I have the signed original of this document which is available for inspection during normal business hours by the Court or a party to this action.

*Declaration electronically signed, pursuant to U.C.A. § 46-4-201(4) and District Of Utah CM/ECF and E-filing guidelines)